AMENDMENTS TO THE SPECIFICATION

Please replace the Abstract with the following:

A block-cipher based encryption scheme providing both privacy and authenticity that encrypts an arbitrary-length message into a minimal-length ciphertext. In one embodiment, "OCB", a message is encrypted using a nonce by partitioning it into 128-bit message blocks and a possibly shorter message fragment. A sequence of offsets is computed from the nonce and block cipher using shifts and conditional xors. Each message block is xored with an offset, enciphered, and xored with the offset, yielding a ciphertext block. The length of the message fragment is encoded, xored with an offset, enciphered to give a pad, truncated, and xored with the message fragment to give a ciphertext fragment. A checksum is formed by xoring the message blocks, the padded ciphertext fragment, and the pad. It is xored with an offset and enciphered to yield a tag. The ciphertext is the ciphertext blocks, the ciphertext fragment, and the tag.